Web安全主题

SQL注入攻击防范

实操手册

2022年8月7日

目录

[一、 手动SQL注入练习 3](#_Toc22042)

[单引号报错注入 3](#_Toc18689)

[基于报错回显 4](#_Toc31363)

[“万能密码”登录 4](#_Toc4039)

[基于布尔的盲注 5](#_Toc14671)

[基于时间的盲注 5](#_Toc3248)

[基于dnslog的盲注 6](#_Toc16082)

[联合查询注入 7](#_Toc3855)

[堆叠查询注入 7](#_Toc26652)

[绕过注释过滤注入 8](#_Toc18070)

[绕过逻辑运算过滤注入 8](#_Toc22901)

[绕过空格过滤注入 9](#_Toc5218)

[绕过union和select过滤注入 9](#_Toc19885)

[二、 工具SQL注入练习 10](#_Toc21889)

[检测是否存在注入 10](#_Toc3351)

[指定注入点、DBMS进行检测 11](#_Toc31377)

[从日志文件发起检测 11](#_Toc12577)

[获取数据库名、数据库表、数据库字段 12](#_Toc7527)

[获取数据库中的数据 12](#_Toc16871)

[运行自定义sql语句 13](#_Toc3296)

[获取数据库所有用户 14](#_Toc25915)

[获取并破解数据库密码 14](#_Toc18506)

[读取系统文件 15](#_Toc21228)

[写入系统文件 15](#_Toc28425)

[执行系统命令 16](#_Toc8282)

[三、 SQL加固练习 17](#_Toc3678)

[关键词过滤 17](#_Toc17816)

[参数校验 17](#_Toc18051)

[预编译查询 18](#_Toc4267)

[关闭报错信息显示 19](#_Toc18798)

[禁用高危函数 19](#_Toc8097)

[降低账号权限 20](#_Toc2307)

# 手动SQL注入练习

## 单引号报错注入

|  |
| --- |
| **实操题目** |
| 单引号报错注入 |
| **实操目的** |
| 学员能够掌握通过一种简单的方法快速检测目标系统是否存在SQL注入漏洞 |
| **实操步骤** |
| 1. 目标链接http://ip/sqli-labs/Less-1/ 2. 通过正常访问方式查看Dumb用户的密码 3. 通过单引号报错方式检测该链接是否存在SQL注入漏洞 |
| **实操过程记录及截图（需要记录漏洞利用参数、操作命令）** |
| 1. 通过正常访问方式查看Dumb用户的密码http://ip/sqli-labs/Less-1/?id=1      1. 访问http://ip/sqli-labs/Less-1/?id=1'出现报错，说明存在漏洞 |

## 基于报错回显

|  |
| --- |
| **实操题目** |
| 基于报错回显 |
| **实操目的** |
| 学员能够掌握基于报错回显方式注入 |
| **实操步骤** |
| 1. 目标链接http://ip/sqli-labs/Less-1/ 2. 采用报错回显方式，获取当前数据库版本 |
| **实操过程记录及截图（需要记录漏洞利用参数、操作命令）** |
| 访问/sqli-labs/Less-1/?id=1' union select 1,updatexml(1,concat(0x7e,version()),1) -- 1 |

## “万能密码”登录

|  |
| --- |
| **实操题目** |
| “万能密码”登录 |
| **实操目的** |
| 学员能够掌握在不知道密码的情况下，利用“万能密码”登录到目标系统 |
| **实操步骤** |
| 1. 目标链接http://ip/sqli-labs/Less-11/ 2. 使用随机一个密码登录admin用户，登录失败 3. 使用“万能密码”登录admin用户，登录成功 |
| **实操过程记录及截图（需要记录漏洞利用参数、操作命令）** |
| * 万能密码为passwd=1' or username='admin' -- 1 |

## 基于布尔的盲注

|  |
| --- |
| **实操题目** |
| 基于布尔的盲注 |
| **实操目的** |
| 学员能够掌握基于布尔的盲注方式 |
| **实操步骤** |
| 1. 目标链接http://ip/sqli-labs/Less-8/ 2. 对目标链接进行测试，测试逻辑“真”，查看页面返回数据 3. 对目标链接进行测试，测试逻辑“假”，查看页面返回数据 4. 判断目标链接是否存在漏洞 5. 测试目标数据库名的长度 |
| **实操过程记录及截图（需要记录漏洞利用参数、操作命令）** |
|  |

## 基于时间的盲注

|  |
| --- |
| **实操题目** |
| 基于时间的盲注 |
| **实操目的** |
| 学员能够掌握基于时间的盲注方式 |
| **实操步骤** |
| 1. 目标链接http://ip/sqli-labs/Less-9/ 2. 对目标链接进行测试，加入时间延迟语句，验证目标链接是否存在漏洞 3. 基于时间盲注，测试目标数据库名的长度 |
| **实操过程记录及截图（需要记录漏洞利用参数、操作命令）** |
|  |

## 基于dnslog的盲注

|  |
| --- |
| **实操题目** |
| 基于dnslog的盲注 |
| **实操目的** |
| 学员能够掌握基于dnslog的盲注方式 |
| **实操步骤** |
| 1. 目标链接http://127.0.0.1/Less-1/（windows环境） 2. 访问http://dnslog.cn获取一个子域 3. 对目标链接进行测试，基于dnslog方式，获取当前数据库名称 4. 基于dnslog方式，获取security.users表中的stupid用户密码 5. 基于dnslog方式，获取security数据库所有的表名 |
| **实操过程记录及截图（需要记录漏洞利用参数、操作命令）** |
|  |

## 联合查询注入

|  |
| --- |
| **实操题目** |
| 联合查询注入 |
| **实操目的** |
| 学员能够掌握联合查询的注入方式 |
| **实操步骤** |
| 1. 目标链接http://ip/sqli-labs/Less-1/ 2. 通过联合查询，获取数据库root用户的密码hash（必须root用户，不需要解密成明文） |
| **实操过程记录及截图（需要记录漏洞利用参数、操作命令）** |
|  |

## 堆叠查询注入

|  |
| --- |
| **实操题目** |
| 堆叠查询注入 |
| **实操目的** |
| 学员能够掌握堆叠查询的利用方式 |
| **实操步骤** |
| 1. 目标链接：http://ip/sqli-labs/Less-38/ 2. 将Angelina用户的密码修改为自己姓名的拼音 3. 查看修改之后的Angelina用户密码 |
| **实操过程记录及截图（需要记录漏洞利用参数、操作命令）** |
|  |

## 绕过注释过滤注入

|  |
| --- |
| **实操题目** |
| 绕过注释过滤注入 |
| **实操目的** |
| 学员能够掌握绕过注释过滤的注入方式 |
| **实操步骤** |
| 1. 目标链接http://ip/sqli-labs/Less-23/ 2. 绕过该链接的限制，执行SQL注入 |
| **实操过程记录及截图（需要记录漏洞利用参数、操作命令）** |
|  |

## 绕过逻辑运算过滤注入

|  |
| --- |
| **实操题目** |
| 绕过逻辑运算过滤注入 |
| **实操目的** |
| 学员能够掌握绕过逻辑运算过滤的注入方式 |
| **实操步骤** |
| 1. 目标链接：http://ip/sqli-labs/Less-25/ 2. 绕过该链接的限制，执行SQL注入 |
| **实操过程记录及截图（需要记录漏洞利用参数、操作命令）** |
|  |

## 绕过空格过滤注入

|  |
| --- |
| **实操题目** |
| 绕过空格过滤注入 |
| **实操目的** |
| 学员能够掌握绕过空格过滤的注入方式 |
| **实操步骤** |
| 1. 目标链接：http://ip/sqli-labs/Less-26b/ 2. 绕过该链接的限制，执行SQL注入 |
| **实操过程记录及截图（需要记录漏洞利用参数、操作命令）** |
|  |

## 绕过union和select过滤注入

|  |
| --- |
| **实操题目** |
| 绕过union和select过滤注入 |
| **实操目的** |
| 学员能够掌握绕过union和select过滤的注入方式 |
| **实操步骤** |
| 1. 目标链接：http://ip/sqli-labs/Less-27b/ 2. 绕过该链接的限制，执行SQL注入，查询到数据库root用户的密码hash |
| **实操过程记录及截图（需要记录漏洞利用参数、操作命令）** |
|  |

# 工具SQL注入练习

## 检测是否存在注入

|  |
| --- |
| **实操题目** |
| 检测是否存在注入 |
| **实操目的** |
| 学员能够掌握通过sqlmap检测目标链接是否存在注入 |
| **实操步骤** |
| 1. 目标链接：http://ip/sqli-labs/Less-1/ 2. 通过sqlmap检测目标链接是否存在注入 |
| **实操过程记录及截图（需要记录漏洞利用参数、操作命令）** |
|  |

## 指定注入点、DBMS进行检测

|  |
| --- |
| **实操题目** |
| 指定注入点、DBMS进行检测 |
| **实操目的** |
| 学员能够掌握通过sqlmap指定注入点、DBMS进行检测，减少检测时间 |
| **实操步骤** |
| 1. 目标链接：http://ip/sqli-labs/Less-1/ 2. 通过sqlmap指定注入点、DBMS进行检测 |
| **实操过程记录及截图（需要记录漏洞利用参数、操作命令）** |
|  |

## 从日志文件发起检测

|  |
| --- |
| **实操题目** |
| 从日志文件发起检测 |
| **实操目的** |
| 学员能够掌握通过burpsuite日志+sqlmap发起SQL注入检测 |
| **实操步骤** |
| 1. 目标链接：http://ip/sqli-labs/Less-1/ 2. 浏览器设置代理指向burpsuite，访问目标链接 3. 从burpsuite中复制出请求日志，保存到文件中 4. sqlmap从日志文件发起检测 |
| **实操过程记录及截图（需要记录漏洞利用参数、操作命令）** |
|  |

## 获取数据库名、数据库表、数据库字段

|  |
| --- |
| **实操题目** |
| 获取数据库名、数据库表、数据库字段 |
| **实操目的** |
| 学员能够掌握通过sqlmap获取数据库名、数据库表、数据库字段 |
| **实操步骤** |
| 1. 目标链接：http://ip/sqli-labs/Less-1/ 2. 通过sqlmap获取当前数据库名 3. 通过sqlmap获取当前数据库表 4. 通过sqlmap获取当前数据库字段 |
| **实操过程记录及截图（需要记录漏洞利用参数、操作命令）** |
|  |

## 获取数据库中的数据

|  |
| --- |
| **实操题目** |
| 获取数据库中的数据 |
| **实操目的** |
| 学员能够掌握通过sqlmap获取数据库中的数据 |
| **实操步骤** |
| 1. 目标链接：http://ip/sqli-labs/Less-1/ 2. 通过sqlmap --dump方式获取mysql数据库中user表的数据 |
| **实操过程记录及截图（需要记录漏洞利用参数、操作命令）** |
|  |

## 运行自定义sql语句

|  |
| --- |
| **实操题目** |
| 运行自定义sql语句 |
| **实操目的** |
| 学员能够掌握通过sqlmap运行自定义sql语句 |
| **实操步骤** |
| 1. 目标链接：http://ip/sqli-labs/Less-1/ 2. 通过sqlmap运行自定义sql语句，查询security数据库中的emails表的数据 |
| **实操过程记录及截图（需要记录漏洞利用参数、操作命令）** |
|  |

## 获取数据库所有用户

|  |
| --- |
| **实操题目** |
|  |
| **实操目的** |
| 学员能够掌握通过sqlmap获取数据库所有用户 |
| **实操步骤** |
| 1. 目标链接：http://ip/sqli-labs/Less-1/ 2. 通过sqlmap获取数据库所有用户 |
| **实操过程记录及截图（需要记录漏洞利用参数、操作命令）** |
|  |

## 获取并破解数据库密码

|  |
| --- |
| **实操题目** |
| 获取并破解数据库密码 |
| **实操目的** |
| 学员能够掌握通过sqlmap获取并破解数据库密码 |
| **实操步骤** |
| 1. 目标链接：http://ip/sqli-labs/Less-1/ 2. 通过sqlmap获取数据库所有用户的密码hash，并破解login用户的明文密码 |
| **实操过程记录及截图（需要记录漏洞利用参数、操作命令）** |
|  |

## 读取系统文件

|  |
| --- |
| **实操题目** |
| 读取系统文件 |
| **实操目的** |
| 学员能够掌握通过sqlmap读取系统文件 |
| **实操步骤** |
| 1. 目标链接：http://ip/sqli-labs/Less-1/ 2. 通过sqlmap读取/etc/passwd文件 |
| **实操过程记录及截图（需要记录漏洞利用参数、操作命令）** |
|  |

## 写入系统文件

|  |
| --- |
| **实操题目** |
| 写入系统文件 |
| **实操目的** |
| 学员能够掌握通过sqlmap写入系统文件 |
| **实操步骤** |
| 1. 目标链接：http://ip/sqli-labs/Less-1/ 2. 编写一个php文件，该文件返回phpinfo()的信息 3. 通过sqlmap，往目标系统的/var/www/html目录写入该php文件 4. 通过浏览器访问该上传的文件 |
| **实操过程记录及截图（需要记录漏洞利用参数、操作命令）** |
|  |

## 执行系统命令

|  |
| --- |
| **实操题目** |
| 执行系统命令 |
| **实操目的** |
| 学员能够掌握通过sqlmap执行系统命令 |
| **实操步骤** |
| 1. 目标链接：http://ip/sqli-labs/Less-1/ 2. 通过sqlmap进入执行系统命令的模式 3. 执行ifconfig命令 4. 执行id命令 |
| **实操过程记录及截图（需要记录漏洞利用参数、操作命令）** |
|  |

# SQL加固练习

## 关键词过滤

|  |
| --- |
| **实操题目** |
| 关键词过滤 |
| **实操目的** |
| 学员能够掌握通过关键词过滤方式进行加固 |
| **实操步骤** |
| 1. 目标链接：http://ip/sqli-labs/Less-1/ 2. 通过联合查询方式测试该链接存在sql注入漏洞 3. 通过修改代码/var/www/html/sqli-labs/Less-1/index.php过滤联合查询的关键词 4. 再次测试是否存在漏洞 |
| **实操过程记录及截图（需要记录漏洞利用参数、操作命令）** |
|  |

## 参数校验

|  |
| --- |
| **实操题目** |
| 参数校验 |
| **实操目的** |
| 学员能够掌握通过参数校验方式进行加固 |
| **实操步骤** |
| 1. 目标链接：http://ip/sqli-labs/Less-1/ 2. 通过联合查询方式测试该链接存在sql注入漏洞 3. 通过修改代码/var/www/html/sqli-labs/Less-1/index.php对传入参数进行合法性校验（白名单方式，需要提供两种加固方式） 4. 再次测试是否存在漏洞 |
| **实操过程记录及截图（需要记录漏洞利用参数、操作命令）** |
|  |

## 预编译查询

|  |
| --- |
| **实操题目** |
| 预编译查询 |
| **实操目的** |
| 学员能够掌握通过预编译方式进行加固 |
| **实操步骤** |
| 1. 目标链接：http://ip/sqli-labs/Less-1/ 2. 通过联合查询方式测试该链接存在sql注入漏洞 3. 通过修改代码/var/www/html/sqli-labs/Less-1/index.php，将sql查询改为预编译方式 4. 再次测试是否存在漏洞 |
| **实操过程记录及截图（需要记录漏洞利用参数、操作命令）** |
|  |

## 关闭报错信息显示

|  |
| --- |
| **实操题目** |
| 关闭报错信息显示 |
| **实操目的** |
| 学员能够掌握通过方式进行加固 |
| **实操步骤** |
| 1. 目标链接：http://ip/sqli-labs/Less-1/ 2. 采用报错回显方式获取当前数据库名 3. 通过修改代码/var/www/html/sqli-labs/Less-1/index.php，屏蔽报错信息 4. 再次尝试注入 |
| **实操过程记录及截图（需要记录漏洞利用参数、操作命令）** |
|  |

## 禁用高危函数

|  |
| --- |
| **实操题目** |
| 禁用高危函数 |
| **实操目的** |
| 学员能够掌握通过禁用高危函数方式进行加固 |
| **实操步骤** |
| 1. 目标链接：http://ip/sqli-labs/Less-1/ 2. 尝试用sqlmap读取/etc/passwd文件内容 3. 禁用文件操作权限 4. 重新读取/etc/passwd文件内容（温馨提示：再次测试时，需要用--flush-session清空会话，否则会有缓存数据） |
| **实操过程记录及截图（需要记录漏洞利用参数、操作命令）** |
|  |

## 降低账号权限

|  |
| --- |
| **实操题目** |
| 降低账号权限 |
| **实操目的** |
| 学员能够掌握通过降低账号权限方式进行加固 |
| **实操步骤** |
| 1. 目标链接：http://ip/sqli-labs/Less-1/ 2. 尝试通过sqlmap获取数据库密码hash 3. 修改/var/www/html/sqli-labs/sql-connections/db-creds.inc文件将数据库用户改成login 4. 再次尝试通过sqlmap获取数据库密码hash（温馨提示：再次测试时，需要用--flush-session清空会话，否则会有缓存数据） 5. 尝试往目标根目录/写入一个test.php文件（原本数据库进程以mysql用户运行，没有权限写入） |
| **实操过程记录及截图（需要记录漏洞利用参数、操作命令）** |
|  |